LISTING OF CLAIMS

1. (currently amended) A method for prohibiting access to a computer after a security device has been removed from said computer, comprising the steps of:

(a) storing data indicating that said security device was originally attached to said computer in a first region of first storage means in said computer;

(b) starting a procedure for prohibiting the access to change said stored data at said computer following the completion of said step (a);

(c) using said data stored in said first region to verify ~~detect~~ that said security device was once attached to said computer;

(d) dynamically determining ~~detecting~~ that said security device ~~has been removed from~~ is no longer attached to said computer; and

(e) prohibiting the access to said computer in response to said steps (c) and (d).

2. (original) The method according to claim 1, wherein said step (b) is initiated in response to a trigger event.

3. (original) The method according to claim 1, wherein said step (e) is performed only when an authorized password is not entered.

4. (currently amended) The method according to claim 3 ~~claim 1~~, further comprising the step of:

~~(e)~~ storing, in response to receipt of an authorized password ~~said steps (c) and (d)~~, data indicating that said security device that was once attached to said computer has been removed in a second region of said first storage means ~~prior to said prohibiting~~.

5. (canceled)

6. (currently amended) A method for prohibiting access to a computer after a security device has been removed from said computer, comprising the steps of:

(a) storing data indicating that said security device was once attached to said computer in a first region of first storage means in said computer;

(b) permitting a central processing unit in said computer to monitor periodically to determine whether said security device is still attached to ~~has been removed from~~ said computer; ~~and~~

(c) determining if an authorized password has been entered;

(d) permitting access to said computer when an authorized password has been entered; and

(e) prohibiting the access to said computer in response to said step (b) when it is determined that an authorized password has not been entered.

7. (currently amended) A computer capable of having a security device removably installed therein, comprising:

first storage means capable of storing data while a main power source of said computer is turned off;

a central processing unit; and

second storage means storing a program that permits said computer to perform the steps of:

(a) storing data indicating that said security device was once attached to said computer in a first region of the first storage means in said computer;

(b) starting a procedure for prohibiting access to change said stored data in said computer following the completion of said step (a);

A1

(c) using said data stored in said first region to detect that said security device was once attached to said computer;

(d) detecting that said security device has been removed from said computer; and

(e) prohibiting the access to said computer in response to said steps (c) and (d).

8. The computer according to claim 7 wherein the second storage means additionally permits the computer to perform the steps of determining whether removal of said security device was authorized, and ~~step of (e)~~ storing, in response

to said determination ~~steps (c) and (d),~~ data indicating that said security device that was once attached to said computer has been legitimately removed in a second region of said first storage means.

9. (currently amended) A computer capable of having a security device removably installed therein, comprising:

first storage means capable of storing data while a main power source of said computer is turned off;

a central processing unit; and

second storage means storing a program that permits said computer to perform the steps of:

(a) storing data indicating that said security device was once attached to said computer in a first region of the first storage means in said computer;

(b) causing ~~causnig~~ the central processing unit in said computer to periodically monitor to determine whether said security device has been removed from said computer; and

(c) prohibiting access to said computer in response to a determination in step (b) that the security device has been removed.

10. (original) A computer capable of having a security device removably installed therein, comprising:

first storage means capable of storing data while a main power source of said computer is turned off;

a central processing unit;

means for storing data indicating that said security device was attached to said computer in a first region of the first storage means;

first detection means for using said data stored in said first region to detect that said security device was once attached to said computer;

second detection means for detecting that said security device has been removed from said computer; and

means for prohibiting access to said computer in response to said detection means.

11. (currently amended) The computer according to claim 10 further comprising means for determining if removal of said security device was authorized and means for storing, in response to said determination ~~first and said second detection means~~ data indicating that said security device that was once attached to said computer has been legitimately removed therefrom in a second region of said first storage means~~; and~~

~~means for prohibiting, in response to said data stored in said second region, access to said computer~~.

12. (original) A computer capable of having a security device removably installed therein, comprising:

first storage means capable of storing data while a main power source of said computer is turned off;

a central processing unit;

means for storing data indicating that said security device that was once attached to said computer has been removed therefrom in a region of the first storage means;

detection means for using said data stored in said region to detect that said security device attached to said computer has been removed therefrom; and

means for prohibiting, in response to said detection means, access to said computer.

13. (canceled)

14. The computer according to claim 7, wherein said first storage means is an RFID tag used by an RFID system, and said security device is an RF antenna.

15. The computer according to claim 8, wherein said first storage means is an RFID tag used by an RFID system, and said security device is an RF antenna.

16. The computer according to claim 9, wherein said first storage means is an RFID tag used by an RFID system, and said security device is an RF antenna.

17. The computer according to claim 10, wherein said first storage means is an RFID tag used by an RFID system, and said security device is an RF antenna.

18. The computer according to claim 11, wherein said first storage means is an RFID tag used by an RFID system, and said security device is an RF antenna.

19. The computer according to claim 12, wherein said first storage means is an RFID tag used by an RFID system, and said security device is an RF antenna.

20. (canceled)

21. The computer according to claim 14, wherein said RF antenna is attached to a lid of a device bay of said computer.

22. The computer according to claim 15, wherein said RF antenna is attached to a lid of a device bay of said computer.

23. The computer according to claim 16, wherein said RF antenna is attached to a lid of a device bay of said computer.

A1

24. The computer according to claim 17, wherein said RF antenna is attached to a lid of a device bay of said computer.

25. The computer according to claim 18, wherein said RF antenna is attached to a lid of a device bay of said computer.

26. The computer according to claim 19, wherein said RF antenna is attached to a lid of a device bay of said computer.

A1

27. (canceled)

28. (new) The method according to claim 1 wherein said storing is done in response to receipt of an RF excitation signal received from a remote RF transmitter.

A2

29. (new) The method according to claim 6 wherein said storing is done in response to receipt of an RF excitation signal received from a remote RF transmitter.

30. (new) The method according to claim 6 further comprising, upon determining that an authorized password has been entered, storing in a second region of said first storage means additional data indicating that said security device that was once attached to the computer has been legitimately removed.